METHODS AND APPARATUS TO PROVIDE SECURE FIRMWARE STORAGE AND SERVICE ACCESS

ABSTRACT

Methods and apparatus to provide secure firmware storage and service access are disclosed. One example method may include receiving a request to execute an instruction in a pre-boot environment, determining an identity of the instruction, determining if an access control list includes an entry corresponding to the instruction, and selectively allowing the execution of the instruction if the access control list includes an entry corresponding to the instruction.